BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-114

13 MAY 2004

Incorporating Through Change 2, 23 OCTOBER 2008

AIR FORCE MATERIEL COMMAND Supplement

4 MAY 2011

Communications and Information

SOFTWARE MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFCA/ITXD (MSgt Robert C. Lowry)

Certified by: USAF/ILC (Col Ronnie D. Hawkins, Jr.)

Pages: 25

Supersedes: AFI33-114, 1 July 2000.

(AFMC)

OPR: HQ AFMC/A6OK

Certified by: HQ AFMC/A6O (Bret Stoneking)

Supersedes: AFI33-114_AFMCSUP1, 18 November 2001

Pages:7

This Air Force instruction (AFI) implements Executive Order (E.O.) 13103, *Computer Software Piracy*, September 30, 1998; Department of Defense Directive (DoDD) 3405.1, *Computer Programming Language Policy*, April 2, 1987; and Air Force Policy Directive (AFPD) 33-1, *Information Resource Management*. It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force (other than software internal to a weapon system; see AFPD 63-1, *Acquisition System*). Send recommended changes and conflicts between this and other publications, using Air Force (AF) Form 847, **Recommendation for Change of Publication**, to HQ AFCA/EASD, with an information copy to the Office of the Secretary of the Air Force, Warfighter Systems Integration and Deployment Directorate, Ground Networks, (SAF/XCDIG), 1800 Air Force Pentagon, Washington DC 20330-1800. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records,* and disposed of in accordance with Air Force Records Information Management

System (AFRIMS) Records Disposition Schedule (RDS). Reference path on AF portal: **https://www.my.af.mil/gcss-af61a/afrims/afrims**. Refer to **Attachment 1** for a glossary of references and supporting information.

(AFMC) This supplement has been developed to assist in complying with AFI 33-114, Software Management. It includes policy and management structure for establishing and managing commercial off-the-shelf software licenses and ensuring are in compliance with the Copyright Act and Executive Order 13103. It clarifies Communications Commanders and Directors involvement in the AFMC Computer Software Licensing Program and also establishes new Base Software License Manager, Unit Software License Manager, Client Systems Technician/Helpdesk, Trusted-User, and Computer User responsibilities. It does not apply to the Air Force Reserve Command nor Air National Guard units. Changes to the procedures in this publication are not authorized without approval of AFSPC/LCMW. The reporting requirements in this AFI are exempt from licensing in accordance with AFI 33-324, paragraph 2.11.10., *The Information Collections and Reports Management Program Controlling Internal, Public, and Interagency Air Force Information Collections.* Submit recommendations for improvements and/or changes in writing to AFMC/A6O, 4225 Logistic Avenue, Wright-Patterson AFB, Ohio 45324. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://www.my.af.mil/afrims/afrims/afrims/rds/rds_series.cfm**

SUMMARY OF CHANGES

This change incorporates interim change (IC) 2 and is the result of an Air Force audit requesting additional wording be inserted to clarify the guidance on actions to take when purchasing COTS software; updates Section B, *Responsibilities*, and Section C, *Installation-Level Software Management*, and updates office symbols.

(AFMC) This document has been substantially revised and must be completely reviewed. This supplement provides major rewrites with AFI 33-114, Software Management.

Section A—Introduction 3

1. Purpose. 3
2. Objectives. 3

Section B—Responsibilities 3

3. Secretary of the Air Force, Warfighter Systems Integration and Deployment Directorate (SAF/XCD). 3
4. Major Command (MAJCOM), Direct Reporting Unit (DRU), Field Operating Agency (FOA), ... 4
5. Headquarters Air Force Communications Agency. 5
6. Headquarters Air Force Materiel Command. 6

7. Headquarters Air Education and Training Command. 6
8. Individual Commercial Off-The-Shelf Software Users. 6
Section C—Installation-Level Software Management 6
9. Managing Licensed Commercial Off-The-Shelf Software. 6
10. Software Developed Using Commercial Off-The-Shelf Office SoftwareTools. ... 8
11. Command, Control, Communications, Computers, and Intelligence (C4I) Software Development; Reuse; and Release. 9
12. Software Configuration, Change, and Release Management. 10
13. Information Assurance. 10
14. Open Systems Guidelines. 10
15. Software Reuse. 10
16. Deleted. 11
17. Bandwidth. 11
18. Checklists. 11
19. (Added-AFMC) AFMC Software License Management Program. 11
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 17
Attachment 2—RELEASE OF SOFTWARE 23

Section A—Introduction

1. Purpose. This instruction provides the guidance and procedures that personnel must use to plan, develop, use, maintain, or support Air Force software to effectively and efficiently complete their assigned missions. It applies to Air Force-procured COTS software and software developed for unique Air Force purposes (other than software internal to a weapon system; see AFPD 63-1).

2. Objectives.

2.1. Gives commanders and users of software at all levels guidance for managing licensed and other software used by Air Force personnel.

2.2. References requirements for standardizing documentation and implementation processes.

Section B—Responsibilities

3. Secretary of the Air Force, Warfighter Systems Integration and Deployment Directorate (SAF/XCD).

3.1. Establishes and oversees computer software management regulatory and policy guidelines.

3.2. Implements Federal Chief Information Officers Council's recommendations for Air Force acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software.

3.3. Ensures compliance with DoDD 8320.1, *DoD Data Administration*, September 26, 1991.

3.4. Establishes criteria for formal licensed software management courses identified by SAF/XCDI in coordination with Headquarters Air Education and Training Command (HQ AETC/SCX).

4. Major Command (MAJCOM), Direct Reporting Unit (DRU), Field Operating Agency (FOA), and Organizational Commanders.

4.1. All MAJCOM/DRU/FOA communications and information systems officers (CSO), where assigned, or commanders representatives where not assigned, will:

4.1.1. Conduct and document an annual inventory of licenses as required by E.O. 13103.

4.1.2. Establish a process to track licenses (see paragraph **9.**).

4.1.3. Develop performance measurements and metrics for software license requirements as required by E.O. 13103.

4.1.4. Identify enterprise software license requirements and management training requirements not covered in existing courses to SAF/XCDI.

4.2. Air Force personnel are to contact the responsible functional or program management office before purchasing software licenses to determine if COTS software licenses are available, or if there is a standard product to buy. Reference path on AF portal: Air Force\Enterprise IT Initiatives\Enterprise COTS Software Agreements.

4.3. Air Force personnel are to coordinate with the Air Force Materiel Command (AFMC) designated product center to obtain volume pricing for products available through the DoD Enterprise Software Initiative (ESI). The Defense Federal Acquisition Regulation (DFAR) Supplement, Part 208, *Required Sources of Supplies and Service*, Subpart 208.74, *Enterprise Software Agreements (ESA)*, requires purchasers to first consider DoD Enterprise Software Agreements found at **https://www.esi.mil**.

4.4. Coordinate with the host communications unit or servicing Network Control Center before implementing any software.

4.5. **(Added-AFMC)** Designate a primary and alternate Command Software License Manager (CSLM) in HQ AFMC/A6O (Operations Division) to develop and manage the Command software license program (CSLM). The primary CSLM responsibilities are outlined in subparagraphs 4.5.1 through 4.5.3 of this supplement.

4.5.1. **(Added-AFMC)** Develop software guidelines and the AFMC software management unit inspection checklist that Base Software License Managers (BSLMs) will use to conduct their base software program.

4.5.2. **(Added-AFMC)** Incorporates the software license management program into Command Inspector General reviews.

4.5.3. **(Added-AFMC)** Ensure requirements of Section 1(c) of Executive Order (E.O.) 13103, Computer Software Piracy, are met as indicated in subparagraphs 4.5.3.1 and 4.5.3.2.

4.5.3.1. **(Added-AFMC)** The E.O. requires government contractors and recipients of Federal grants and loans to have "appropriate systems and controls in place to ensure Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws." The E.O. further provides; if any agency becomes aware contractors or recipients are using federal funds to acquire, operate, or maintain unlicensed software and determines such actions may effect the integrity of the agency's contracting and financial assistance processes, the agency is required to "take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law."

4.5.3.2. **(Added-AFMC)** Each agency must take appropriate measures to ensure government contractors and recipients of grants and other federal funding comply with applicable copyright laws, regulations, instructions, directives, E.O.s, Air Force requirements/guidelines, and Air Force Materiel Command (AFMC) requirements/guidelines.

5. Headquarters Air Force Communications Agency.

5.1. Surveys and consolidates MAJCOM, FOA, and DRU requirements for potential Air Force enterprise software licenses for COTS computer and network management software.

5.2. Recommends candidate software products for potential Air Force-wide licensing to the Air Force Materiel Command (AFMC) product center designated with the responsibility for enterprise license management.

5.3. Consolidates new MAJCOM training for managing software licenses (including computer-based initiatives) and sends them to Headquarters Air Education and Training Command (HQ AETC/SCX, 61 Main Circle Suite 2, Randolph AFB TX 78150-4545) for incorporating formal courses or in long-distance learning approaches.

5.4. AFCA Combat Information Transport System (CITS) will implement the Information Technology (IT) Asset & Systems Management (ITASM) which will provide for a USAF-Enterprise Configuration Management Database (CMDB) that will hold information for all USAF COTS entitlements and software implementation metrics. This will be the authoritative source of information for software entitlement and implementation metrics.

5.4.1. AFCA CITS ITASM USAF-Enterprise CMDB will enable Air Force adoption of the International Standardization Bodies/International Electrotechnical Commission (ISO/IEC) 20000, *Information Technology - Service Management*, also known as Information Technology Infrastructure Library practices for Software Asset Management. This will complement ISO/IEC 19770, *Software Asset Management (SAM).*

5.4.2. AFCA CITS ITASM will provide mechanism for USAF-Enterprise Evaluated Approved Products List that will publish to the USAF-Portal the COTS Software Products that have been certified for use on USAF networks.

5.4.3. AFCA CITS ITASM CMDB will publish to DoD ITAM (DoD IT Asset Management) metrics for both software entitlements and implemented software.

5.4.4. CITS ITASM CMDB Initial Operating Capability (IOC) for Network Management Software Entitlements is targeted for December 2009. IOC for Server Software Entitlements is targeted for December 2010, and IOC for Desktop Software Entitlements is targeted for December 2011.

6. Headquarters Air Force Materiel Command.

6.1. Designates a product center as the office of primary responsibility (OPR) for managing the Air Force Enterprise Software License Program and, when designated, acts as executive agent for establishing DoD-wide enterprise software licenses.

6.2. Designates a product center as purchasing agent for software licenses to support consolidated and programmatic Air Force requirements.

6.3. Manages Air Force Enterprise Software Licenses for COTS computer and network management software.

6.4. **(Added-AFMC)** AFMC Software License Management Program. Specific responsibilities under this program are contained in subparagraphs 19.1 through 19.7.2 of this supplement.

7. Headquarters Air Education and Training Command.

7.1. Develops training plans and materials for comprehensive training that addresses all aspects of managing the operation of installation-level licensed software.

7.2. Establishes curricula for formal licensed software management courses identified by SAF/XCDI.

7.3. Provides training through centrally managed computer based training courses or other distance learning approaches.

8. Individual Commercial Off-The-Shelf Software Users.

8.1. Do not install and use copies of government-owned software on a home computer unless the software license explicitly allows users to do so and the base CSO has authorized such use. When authorized for installation on a home computer, only use the software for official Air Force business. Personal use may be a violation of *The Copyright Act*, rendering the individual user accountable and liable.

8.2. Do not install freeware, shareware, or personally owned software on government systems without approval of the system administrator or network manager servicing your organization, according to AFI 33-115V1, *Network Management*; and AFI 33-202, *Computer Security*.

8.3. Do not make any illegal copies of copyrighted software.

Section C—Installation-Level Software Management

9. Managing Licensed Commercial Off-The-Shelf Software. The communications squadron commander or CSO at each installation who implements licensed COTS or other software shall:

9.1. Develop and implement a documented process to ensure that all software (including freeware, shareware, licensed COTS products, and pre-production versions) is free of viruses and malicious logic.

9.2. Annually instruct personnel on licensed software usage; *The Privacy Act* and *The Copyright Act* considerations; and Air Force, DoD and E.O. provisions.

9.3. Register organization ownership of licensed COTS software and ensure an annual inventory is conducted of all licensed COTS software in the organization.

9.4. Use a metering mechanism if licensed for server-hosted, concurrent-user application software to prevent exceeding the authorized number of copies and users. Record network manager or system administrator inventory of licensed client and network software as part of the annual installation licensed software inventory.

9.5. Maintain a record of the COTS software controlled by the organization.

9.6. Store evidence (e.g., user manual, purchase documentation, compact disk, etc.) of licenses in a secure location (e.g., a locked file cabinet).

9.7. Dispose of old versions of COTS software according to licensing agreements. Upgrades from the original software source are normally considered a continuation of the original license, not an additional or new license.

9.8. Redistribute excess or superseded COTS software if it:

9.8.1. Is allowed under the license agreement or upgrade policy for that software.

9.8.2. Is not classified.

9.8.3. Did not provide direct security protection to automated data processing equipment in systems that processed classified information.

9.8.4. Is not directly related to or associated with a weapon system, intelligence system, command and control system, communications system, or tactical system.

9.8.5. Still operates as intended.

9.9. Dispose of excess or superseded COTS software not redistributed by one of the following methods:

9.9.1. Return the software package (distribution media, manuals, etc.) to the company that developed the software.

9.9.2. Destroy the software according to the provisions of the licensing agreement. (***NOTE:*** Document the method of destruction to establish an audit trail.) This may include:

9.9.2.1. Destroying the documentation and distribution media.

9.9.2.2. Formatting or erasing the master floppy disks.

9.9.2.3. Using the master floppy disks as scratch disks.

9.9.3. Audit all computer and server software annually to ensure there are no illegal or unauthorized copies of COTS or other software installed. Sampling procedures may be used if active inventorying is available.

9.10. Installations that deploy and manage COTS software shall utilize ITASM to track software entitlements and implementation information.

9.10.1. Installations are to utilize AutoDiscovery Tools to acquire implemented software information that is to be reported by the ITASM system. Installations are to utilize CITS ITASM standard tools where applicable. AutoDiscovery Tools will suffice for audit on implemented software on network attached computers and servers.

9.10.2. Installations utilization of ITASM will complement the AFCA CITS ITASM deployment schedule.

10. Software Developed Using Commercial Off-The-Shelf Office SoftwareTools. Air Force computer users are encouraged and expected to use their licensed COTS office software to increase their individual professional productivity and overall unit effectiveness. Users must coordinate networked or "group" computer applications that are user built with these tools with the installation CSO. This precludes later impact on network and server capacity, avoids duplication of effort on similar application software within the installation or MAJCOM, and ensures continued software support after departure of one or more of the original user-developers. Air Force user-developers shall:

10.1. Ensure the Air Force retains property rights to the computer software developed in the course of their duties.

10.2. Not by-pass computer/network server operating systems, security systems, or access controls provided by higher authority.

10.3. Provide the CSO a software documentation package in appropriate digital format. The software package must include:

10.3.1. The author or point of contact, organization, and telephone number.

10.3.2. A descriptive unclassified title with version number as the first delivery (use Version 1.0).

10.3.3. A brief (one paragraph) unclassified description of the software's functionality for use in publishing software reuse catalogs; and a classified description, if necessary, to more fully explain the software's capabilities.

10.3.4. A brief description of all testing (such as Year 2000) performed on the mission application software and its databases.

10.3.5. A brief user's guide. The user's guide should include:

10.3.5.1. The hardware configuration required.

10.3.5.2. The supporting software required to include the operating system and (if any) supporting COTS software with version release number.

10.3.5.3. Compiling and linking instructions, if applicable.

10.3.5.4. Descriptions of the software installation process, required hardware setup, menus, and software capabilities and functions.

10.3.5.5. Samples of terminal output screens and print products produced (if any).

10.3.5.6. Other information useful for continued effective use and maintenance of the mission application software.

11. Command, Control, Communications, Computers, and Intelligence (C4I) Software Development; Reuse; and Release. Adhere to DoDD 3405.1; DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 12, 1992; DoD Instruction (DoDI) 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 18, 1992; and Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01A, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 June 1995; when developing mission or application software for C4I systems.

11.1. Organic Development. Do not develop software organically unless quality, cost, performance, schedule, or interoperability requirements cannot be met with COTS or non-developmental item software.

11.1.1. Acquire an approved mission needs statement before developing organic software requiring over 6 man-months of effort or costing in excess of $50,000, and follow guidance for software acquired under DoD 5000-series acquisitions.

11.1.2. All units that develop or maintain software will have a software process improvement (SPI) program and a documented SPI plan, including at least:

11.1.2.1. A baseline of their current capabilities.

11.1.2.2. Goals and milestones they intend to reach.

11.1.2.3. Metrics to measure their progress toward their goals and milestones.

11.1.2.4. Timeline for SPI appraisals. The Software Technology Support Center (STSC) at Hill Air Force Base UT is available on a fee-recovery basis for SPI appraisals, but any qualified SPI appraiser may be used.

11.1.2.5. Identify life-cycle support requirements for the life of developed software.

11.2. Releasing COTS Office Software Tools. It is Air Force policy to release, upon consideration of a valid written request, specific software developed exclusively with government funds or otherwise owned by the Air Force. The OPR for the software decides to release or disclose that software. The approval authority may be at a higher level depending upon the recipient (e.g., approval authority for all foreign release requests is Secretary of the Air Force [SAF/IADD]). When not for foreign release and the OPR is in doubt regarding the release of software, send the request to HQ USAF/SCX, 1250 Air Force Pentagon, Washington DC 20330-1250, for resolution. *Freedom of Information Act* (FOIA) requests must be sent to the local FOIA manager to control and respond using guidelines in the Air Force supplement to DoD 5400.7-R (DoD 5400.7-R/AFSUP), *DoD Freedom Of Information Act Program*, 22 July 1999. Before releasing the software, the OPR shall require the requester to sign a memorandum of agreement (see **Attachment 2**). Releases of Air Force-owned or developed software from software reuse libraries, or software under Air Force-industry Cooperative Research and Development Agreements (CRADA), are exceptions to this policy.

11.3. When developing mission or application software for information systems, it is desirable to utilize that Software Engineering Institute's Software Capability Maturity Model Integrated (CMMI) as advocated by the Software Technology Support Center (STSC) at Hill AFB UT (**www.stsc.hill.af.mil**), or the 754th Electronic Systems Group's Systems Engineering Process (**www.gunter.af.mil/sw**).

12. Software Configuration, Change, and Release Management. Use ISO/IEC 20000, or ITIL (Information Technology Infrastructure Library), Configuration Management, Change Management, and Release Management processes to plan, identify, control, monitor, verify, and manage software configuration items. Typically, software configuration items would include information such as purchase order number, purchase date, software manufacturer, software title, and version implemented.

13. Information Assurance. Program managers and software developers must integrate information assurance into their systems using guidance contained in AFPD 33-2, *Information Protection* (converting to *Information Assurance*), and the Air Force 33-200 series publications. These publications give policy guidelines for developing and using the computer, communications, and emissions security programs needed for all Air Force communications and information systems.

14. Open Systems Guidelines. The Air Force is committed to meeting the DoD objective of developing interoperable and maintainable systems based on open standards. To that end, system developers, contract administrators, and maintainers must adhere to the guidance given in the DoD Joint Technical Architecture (JTA) and JTA-Air Force (JTA-AF). These documents identify a common set of mandatory information technology standards and guidelines used in all new systems and system upgrades in the DoD. Each unit ensures that upgrades to systems under maintenance comply to the maximum extent possible with the JTA and JTA-AF.

15. Software Reuse. Software reuse is the practice of using existing software components to develop new software applications. Software reuse benefits the Air Force through increased developer productivity, improved quality and reliability of software-intensive systems, enhanced system interoperability, lowered program technical risk, and shortened software development and maintenance time.

15.1. Reusable software components may include executable software binaries, source code segments, program documentation, project plans, requirement descriptions, design and architecture documents, database schemas, test data and test plans, user's manuals, software tools, and object classes. These assets can be most efficiently used when designed and packaged to fit into a product-line architecture at each software development location for a specific mission area or functional domain, using interface standards and common communications protocols. The domain product-line components can then be used to create families of related systems designed to share common software architecture for the domain.

15.2. Each Air Force software development location should:

15.2.1. Establish a software reuse library or repository for internal sharing of the reusable software components developed at the location.

15.2.2. Report each reusable software component to the Air Force Reuse Center, Standard Systems Group, Maxwell AFB-Gunter Annex AL, for storage in the Air Force Defense Software Repository System.

15.2.3. Upon valid written request, release software component using the software release memorandum of agreement at **Attachment 2**.

16. Deleted.

17. Bandwidth. The Air Force is faced with restrictions on the amount of information that can be provided to our forces, particularly in remote areas of the world. Therefore, software systems designers and developers must discipline themselves in the quantity and content of non-mission essential information sent over supporting network infrastructures (that is, ensure sending only operationally necessary data). In addition to DoD direction, follow all policy and procedures in AFIs 33-101, *Communications and Information Management Guidance and Responsibilities*; 33-115V1; 33-119, *Electronic Mail (E-Mail) Management and Use*; and 33-129, *Transmission of Information Via the Internet*; on downloading from the Internet, transmission of e-mail attachments, video teleconferencing, Web browsing, and conservation measures during periods of surge or network degradation. Air Force-developed software (including that developed specifically for the Air Force) will accommodate network infrastructure considerations into its systems design and internal code, such that it does not overtax the infrastructure that it relies and operates.

18. Checklists. Use AF Form 2519, **All Purpose Checklist** (available electronically), to develop a checklist on software and software license management using paragraphs **3.** through **8.**

19. (Added-AFMC) AFMC Software License Management Program. Specific responsibilities under this program are contained in subparagraphs 19.1 through 19.7.2 of this supplement.

19.1. **(Added-AFMC)** Communications Commander (or Director) Responsibilities. Each communications commander/director will comply with subparagraphs 19.1.1 through 19.1.3.

19.1.1. **(Added-AFMC)** Designate primary and alternate Base Software License Managers (BSLMs) to manage the wing and base software license programs. Commanders of AFMC units assigned to non-AFMC bases will appoint an individual to act as BSLM for that unit and manage the software license program if a host BSLM does not already exist. AFMC Communications Commanders (or Directors) that are tenants on an AFMC base may appoint, at their discretion, an individual to act as BSLM for that unit and manage the software license program if a host BSLM does not already exist.

19.1.2. **(Added-AFMC)** Forward BSLM appointment memorandum to HQ AFMC/A6O, CSLM or post a copy on the CSLM SharePoint website link under the assigned BSLM software folder. (**https://cs.eis.afmc.af.mil/sites/AFMC_SLM/BSLM%20Workspace/Forms/AllItems.aspx**)

19.1.3. **(Added-AFMC)** Annually certify and document in writing to the CSLM or post in the BSLM software folder a software inventory was accomplished and the provisions of this AFI have been met. Certifications are due to the CSLM no later than the anniversary date of the BSLM's appointment.

19.2. **(Added-AFMC)** Unit Commanders, Directors, and Division Chiefs of HQ AFMC Directorates Responsibilities. Each unit commander/director will comply with subparagraphs 19.2.1 through 19.2.8.

19.2.1. **(Added-AFMC)** Appoint a primary and alternate Unit Software License Manager (USLM) to administer their unit software license program. Trusted-Users may be appointed if needed.

19.2.2. **(Added-AFMC)** Forward USLM appointment memorandum to the BSLM. Annually update and forward USLMs appointment memo to the BSLM no later than the anniversary date of the USLM's appointment.

19.2.3. **(Added-AFMC)** Ensure outgoing and incoming USLMs conduct a joint inventory of all licensed software and endorse all inventories upon departures.

19.2.4. **(Added-AFMC)** Annually certify and document to the BSLM a software inventory was accomplished. Accomplish this certification by signing the annual inventory list or memorandum and indicate the unit's annual software license inventory has been accomplished. Complete this certification each year no later than the anniversary date of the USLMs appointment.

19.2.5. **(Added-AFMC)** Ensure software acquisitions are coordinated through the respective BSLM prior to purchasing software.

19.2.6. **(Added-AFMC)** Ensure USLM is notified of all deliveries of new software licenses and copies of licensing material is provided to the USLM. Ensure software is added to the unit's software inventory.

19.2.7. **(Added-AFMC)** Ensure necessary training for users is obtained for unique software purchased or developed by units are conducted.

19.2.8. **(Added-AFMC)** Ensure Air Force Enterprise license agreement contracts are used to procure common-user desktop/laptop software on new computer systems and comply with subparagraphs 19.8 through 19.8.2, the Air Force Standard Desktop Configuration (SDC).

19.3. **(Added-AFMC)** BSLM Responsibilities. Each BSLM will comply with subparagraphs 19.3.1 through 19.3.8.

19.3.1. **(Added-AFMC)** Ensure host-tenant support agreement directs all base units to participate in the host-base software license management program if they use Air Force Command, Control, Communications, and Computer (C4) systems or are connected to Air Force local area networks.

19.3.2. **(Added-AFMC)** Place semiannual reminders of the need for proper software license management in base bulletins and other media to increase and reinforce the legal requirement of maintaining software licenses according to their stated conditions.

19.3.3. **(Added-AFMC)** Provide software license training for newly appointed BSLMs, USLMs, and client systems technicians/helpdesks (CSTs). Utilize the base Intranet to the maximum extent possible as a tool to educate all users. This training will include, but should not be limited to, subparagraphs 19.3.3.1 through 19.3.3.5.

19.3.3.1. **(Added-AFMC)** Ensuring all USLMs and CSTs/Helpdesks are familiar with their responsibilities as listed in paragraphs **19.4** and **19.5** of this supplement, and paragraph 9 of the basic AFI 33-114 that covers the disposal of excess or superseded Commercial Off-The-Shelf Software (COTS).

19.3.3.2. **(Added-AFMC)** Ensuring all USLMs and CSTs/Helpdesks are familiar with the Air Force Certificate-to-Operate (CTO) process.

19.3.3.3. **(Added-AFMC)** Ensuring all BSLMs complete the US Air Force Software License Management and Information Assurance Awareness Program training.

19.3.3.4. **(Added-AFMC)** Explaining how to maintain accurate records of installed software licenses. Contact local Functional Area Records Managers or Base Records Management Office to ensure proper retention and disposition of official records and for approval of records in the office file system.

19.3.3.5. **(Added-AFMC)** Legal briefings given under the direction of this AFMC Supplement will be done in coordination with the appropriate JA offices before explaining the basics of software licenses and the Copyright Act.

19.3.4. **(Added-AFMC)** Ensure each unit maintains a software inventory of all government owned GOTS/COTS software in unit use.

19.3.5. **(Added-AFMC)** Ensure each unit performs an annual inventory of all (including non-standard) software licenses, and corresponding documentation of unit software. Ensure unit commander/director endorses and forwards a copy to BSLM.

19.3.6. **(Added-AFMC)** Perform periodic compliance visits to base units and AFMC tenant organizations.

19.3.7. **(Added-AFMC)** Maintain a current list of all USLMs.

19.3.8. **(Added-AFMC)** Ensure automated tools are used to the maximum extent possible for tracking software installed on the base network.

19.4. **(Added-AFMC)** USLM Responsibilities. Each USLM will comply with subparagraphs 19.4.1 through 19.4.13.

19.4.1. **(Added-AFMC)** Become familiar with software license agreements used in organizations.

19.4.2. **(Added-AFMC)** Coordinate with the BSLM, functional system administrators, CSTs/helpdesks, and software purchasers.

19.4.3. **(Added-AFMC)** Monitor delivery of all new software, update software inventory list, inform the BSLM in a timely manner, and become familiar with software license agreements.

19.4.4. **(Added-AFMC)** Store evidence of license agreements or licenses (e.g. user manuals, purchase documentation, CD-ROMs, etc.) and physical software media in a secure centralized location (e.g., locked drawer, file cabinet, room, etc.). Work with local Functional Area Record Manager or Base Records Management Office to ensure proper retention and disposition of official records and records approval in the office file system.

19.4.5. **(Added-AFMC)** Ensure the legal use of all software.

19.4.5.1. **(Added-AFMC)** Each COTS application must have a license.

19.4.5.2. **(Added-AFMC)** Use of software corresponds to the applicable license agreement.

19.4.5.3. **(Added-AFMC)** Ensures user desktops/laptops are in compliance with the AF SDC policies as contained in subparagraphs 19.8 through 19.8.2 of this supplement.

19.4.6. **(Added-AFMC)** Identify software that does not have associated licenses, assemble proofs-of-purchase per paragraph **19.4.11**, and request replacement licenses from publishers, as needed. Develop plan of action to obtain compliance within 120 days.

19.4.7. **(Added-AFMC)** Coordinate training with the BSLM, as needed.

19.4.8. **(Added-AFMC)** Ensure unit's in-processing worksheets require newly assigned personnel receive software license training within 30 days of arrival and annually thereafter NLT the anniversary of initial training. This training will include, but not limited to, items outlined in subparagraphs 19.4.8.1 through 19.4.8.4.

19.4.8.1. **(Added-AFMC)** Promoting user awareness of unauthorized or illegal use of computer software.

19.4.8.2. **(Added-AFMC)** Legal ramifications of failing to take immediate corrective action "upon identifying the presence of illegal software". USLMs should work with their BSLMs and their local JAG office to ensure accuracy in their message before explaining how, and to what extent, a user may be held liable for unauthorized or illegal use of computer software.

19.4.8.3. **(Added-AFMC)** Training users on procedures for acquiring new software.

19.4.8.4. **(Added-AFMC)** Making users aware of the importance of identifying unauthorized or illegal software on their systems and legal ramifications of failing to take immediate corrective action.

19.4.9. **(Added-AFMC)** Circulate software licensing information, as needed, throughout the organization.

19.4.10. **(Added-AFMC)** Support and implement the base software license program.

19.4.11. **(Added-AFMC)** Maintain a hard or soft copy of the software license inventory and "Proof-of-License Ownership" of all government own/COTS software in use within their unit. Proof may consist of hardcopy or softcopy documentation from the supplier such as manual, purchase documentation, email, or distribution media. Inventory must include items outlined in subparagraph **19.4.11.1**.

19.4.11.1. **(Added-AFMC)** "Purchase Data as required" (i. e. Vendor Name, Purchase Order or Delivery Order Number, Description, Version, Cost, Quantity Purchased, License ID Number(s), Funding Data, Date Purchased, Expiration/Renew by Dates).

19.4.11.1.1. **(Added-AFMC)** . Ensure software covered by an enterprise license agreement is not transferred with hardware when performing automated data processing equipment (ADPE) transactions.

19.4.12. **(Added-AFMC)** Perform an annual inventory of all software licenses and cross check with installed software. Complete certification each year no later than the

anniversary date of the USLM's official appointment. Ensure unit commander or director endorses the report.

19.4.13. **(Added-AFMC)** Perform a joint inventory of all software licenses and cross check with installed software before transferring responsibility to another USLM. Ensure unit commander or director endorses the report.

19.5. **(Added-AFMC)** Client Systems Technician/Helpdesk Responsibilities (CST). Each Client Systems Technician/Helpdesk will comply with subparagraphs 19.5.1 through 19.5.4.

19.5.1. **(Added-AFMC)** Notify USLMs of any actions that are performed for a user that changes software licenses installed on their computer system.

19.5.2. **(Added-AFMC)** Do not purchase or obtain software without prior coordination of the USLM.

19.5.3. **(Added-AFMC)** Ensure limited user accesses on NIPRNET Clients are imposed on users computers so the AF SDC in integrity is enforced. Periodic monitoring of users computers can be accomplished by using an automation software tool to ensure administrator rights are removed.

19.5.4. **(Added-AFMC)** Ensure all user computer systems are in compliance with the AF SDC in subparagraphs 19.8 through 19.8.2.

19.6. **(Added-AFMC)** Computer User Responsibilities. Each Computer user will comply with paragraphs 19.6.1 through 19.6.3.

19.6.1. **(Added-AFMC)** Assist USLMs with software inventories on computer as required.

19.6.2. **(Added-AFMC)** Do not make illegal copies of copyrighted software.

19.6.3. **(Added-AFMC)** Ensure user computer systems are in compliance with the AF SDC in subparagraphs 19.8 through 19.8.2.

19.7. **(Added-AFMC)** Trusted-User Responsibilities. "Trusted Users" will comply with subparagraphs 19.7.1 and 19.7.4.

19.7.1. **(Added-AFMC)** Must be appointed by unit commander or director.

19.7.2. **(Added-AFMC)** Will follow all software license requirements outlined for CSTs/Helpdesks and USLMs pertaining to computer system requirements and software license management.

19.7.3. **(Added-AFMC)** Ensure limited user accesses on NIPRNET Clients are imposed on user's computers so the AF SDC is enforced.

19.7.4. **(Added-AFMC)** Ensure personal computer systems are in compliance with the AF SDC in subparagraphs 19.8 through 19.8.2.

19.8. **(Added-AFMC)** The Air Force Standard Desktop Configuration (SDC) Software Implementation provides standard core desktop software and security settings across the AF.

19.8.1. **(Added-AFMC)** It is mandatory that all Windows-based computers have the AF SDC loaded on desktop/laptop computers to provide a secure set of standard applications and preclude unauthorized computer desktop/laptop modifications.

19.8.2. **(Added-AFMC)** Use of the SDC implements Least User Access (LUA) procedures and sharply reduces the need for elevated computer system access rights. Additionally, standardized AF client computers, dramatically reduce administrative workloads and possible compromises. Guidelines can be found under the "AFNOSC NTO 2006-227-201: Implementation of Limited User Access on NIPRNET Clients".

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

(AFMC)

PAUL A. PARKER, SES
Director of Communications,
Installations and Mission Support.

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

E.O. 13103, *Computer Software Piracy,* September 30, 1998

Freedom of Information Act, 5 U.S.C. section 552, as amended by Public Law No. 104-231, 110 Stat. 3048

The Copyright Act

The Information Technology Management Reform Act (Division E of Public Law 104-106)

The Privacy Act

CJCSI 6212.01A, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 June 1995

DFAR Supplement, Part 208, *Requires Sources of Supplies and Services*, Subpart 208.74, *Enterprise Software Agreements*, 25 October 2002

DoDD 3405.1, *Computer Programming Language Policy,* April 2, 1987

DoDD 4630.5, *Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 12, 1992

DoDI 4630.8, *Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems*, November 18, 1992

DoD 5400.7-R/AFSUP, *DoD Freedom of Information Act Program*, 22 July 1999

DoDD 8320.1, *DoD Data Administration*, September 26, 1991

DoD 8320.1-M, *Data Administration Procedures*, March 29, 1994

DoD 8320.1-M-1, *Data Standardization Procedures,* April 2, 1998

ISO/IEC 19770, Software *Asset Management (SAM)*

ISO/IEC 20000, *Information Technology - Service Management*

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFPD 33-1, *Information Resource Management*

AFPD 63-1, *Capability-Based Acquisition System*

AFPD 33-2, *Information Assurance (IA) Program*

AFI 33-101, *Communications and Information Management Guidance and Responsibilities*

AFI 33-115V1, *Network Operations (NETOPS)*

AFI 33-119, *Air Force Messaging*

AFI 33-129, *WEB Management and Internet Use*

AFI 33-202, *Network and Computer Security*

AFMAN 33-363, *Management of Records*

Abbreviations and Acronyms

(Added-AFMC) CST/Helpdesk—Client Systems Technician/Helpdesk

(Added-AFMC) ADPE—Automated Data Processing Equipment

AETC—Air Education and Training Command

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFIND—Air Force Index

AFMC—Air Force Materiel Command

AFPD—Air Force Policy Directive

(Added-AFMC) BSLM—Base Software License Manager

C4—Command, Control, Communications, and Computers

C4I—Command, Control, Communications, Computers, and Intelligence

CITS—Combat Information Transport System

CJCSI—Chairman Joint Chiefs of Staff Instruction

CMDB—Configuration Management Database

COMPUSEC—Computer Security

COTS—Commercial Off-the-Shelf

CRADA—Cooperative Research and Development Agreements

(Added-AFMC) CSLM—Command Software License Manager

CSO—Communications and Information Systems Officer

DFAR—Defense Federal Acquisition Regulation

(Added-AFMC) DITSCAP—DoD Information Technology Security Certification and Accreditation Process

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DRU—Direct Reporting Unit

E.O.—Executive Order

ESA—Enterprise Software Agreement

ESI—Enterprise Software Initiative

FOA—Field Operating Agency

FOIA—Freedom of Information Act

IT—Information Technology

ITASM—IT Asset & Systems Management

ITIL—Information Technology Infrastructure Library

JTA—Joint Technical Architecture

JTA—AF—Joint Technical Architecture-Air Force

MAJCOM—Major Command

OPR—Office of Primary Responsibility

SAF—Secretary of the Air Force

SAM—Software Asset Management

(Added-AFMC) SDC—Standard Desktop Configuration

(Added-AFMC) SMS—Systems Management Server Software

SPI—Software Process Improvement

STSC—Software Technology Support Center

USAF—Headquarters United States Air Force

(Added-AFMC) USLM—Unit Software License Manager

Terms

(Added-AFMC) Accreditation—Formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards and controls.

AutoDiscovery Tool—Applications that can audit computers and services for physical and software configuration information.

Certification—For purposes of this instruction, the act of determining that software performs without defects and viruses, and does what the supporting documentation says it will do in accordance with any specified acceptance criteria.

(Added-AFMC) Client Systems Technician/Helpdesk—Client Support Technician/Helpdesk (CST) is a new term for Client Support Administrator (CSA). Reference: Client Systems & Knowledge Operations Management Workforce Restructure Strategy Memo, 5 October 2009.

(Added-AFMC) This memo requires realignment of the CSAs—This centralizes the CST (formally known as CSA) workforce to provide focused IT desktop support, reduces vulnerabilities to our networks, and migrates towards an enterprise service desk (known as helpdesk).

Command, Control, Communications, and Computer (C4) Systems—Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, across the range of military operations. Also called "communications and information systems."

Commercial Off-The-Shelf (COTS) Software—Software developed, tested, and sold by commercial companies to the general public. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

Communications and Information Systems Officer (CSO)—Identifies the supporting CSO at all levels. At base level, this is the commander of the communications unit responsible for carrying out base communications and information systems responsibilities, the base CSO. Tenant organizations may also have CSOs. At MAJCOM, and other activities responsible for large quantities of communications and information assets, it is the person designated by the commander as responsible for overall management of communications and information assets budgeted and funded by the MAJCOM or activity. The CSO function, when under the base communications unit, uses the office symbol "SC" that expands to three and four digits to identify specific functional areas.

Configuration Management Database (CMDB)—A CMDB is a database that contains all relevant information about the components of the information system used in an organization's IT services and the relationships between those components. Typically includes hardware, software, and topology information.

Computer Security (COMPUSEC)—1. The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. See also "communications security". 2. Measures and controls that ensure confidentiality, integrity, and availability of information systems assets including hardware, software, firmware, and information being processed, stored, and communicated.

Copyright—Without a license that specifies otherwise, the purchaser's use of software is restricted to making an archival copy and installing the computer program onto a single computer, in accordance with the *Copyright Act of 1976*. Do not reproduce or use copyrighted software in any other manner.

Documentation—Records required to plan, develop, operate, maintain, and use electronic records and software. Included are systems specifications, file specifications, code books, record layouts, user guides, and output specifications.

DoD Enterprise Software Initiative (ESI)—A DoD Chief Information Officer-led joint DoD project to develop and implement a DoD enterprise process to save money and improve information sharing on COTS products. The objective is to reduce problems identified with procuring software for DoD (including price, acquisition cost, distribution, training, maintenance, and support) for common-use, standards-compliant software.

Enterprise License—Allows the purchasing organization to use multiple copies of a specific COTS software program, usually up to a specified number, across the organization for a set price. This is usually a more cost-effective acquisition strategy than purchase of individual copies. Either the Air Force Enterprise Software License Program or DoD ESI should be considered for commonly used software.

Enterprise Software Agreement (ESA)—Agreements, such as contracts or blanket purchase agreements, by which organizations acquire software or software maintenance under specified terms and conditions.

Hardware—The physical equipment and devices forming a computer and peripheral components.

Interoperability—The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them

to operate effectively together. The condition achieved among communications-electronics systems or items of communications-electronics equipment when exchanging information or services directly and satisfactorily between them and/or their users.

(Added-AFMC) License Agreement—A contract between the software publisher and the user which instructs and limits how the software is to be used. When software is purchased, the purchaser acquires a license to use it, but the publisher retains full rights to the software and can further distribute and reproduce it. AFMC's license agreements generally fall into one of the following categories:

Enterprise License—The DoD and Air Force Enterprise Software Initiatives (ESI) and the Enterprise software agreements (ESA) entered into by DoD components who manage commercially available software at the DoD Enterprise level to reduce the cost of acquiring and maintaining software products,

Individual License—A license for use on a single machine only.

Network License—license that allows every member of the network to access the software.

Site License—A license defined by a geographic restriction, such as a building, unit, wing, or base.

Trusted-User—Computer users with unique requirements that require administrative privileges. They manage unique computer operations such as modeling and simulation computer systems, standalone systems or computers with unique software/operational requirements.

License Agreements—Contracts between the software publisher and the user that instructs and limits the software use. When purchasing software, the buyer only acquires a license to use it. The publisher retains the full rights to the software and has the sole right to its further distribution and reproduction.

Maintenance—Any job described as one that eliminates faults or keeps hardware or software running in satisfactory working condition falls into the maintenance category. (See AFI 21-116, *Maintenance Management of Communications-Electronics*.)

Network—Two or more computers connected to each other through a multi-user system or by other electronic means to exchange information or share computer hardware or software.

Requirement—A need for a new or improved information processing capability that, when satisfied, increases the probability of operational mission success or decreases the cost of mission support.

Reuse—The process of developing or supporting a software-intensive system using existing software assets. (See DoDD 3405.1.)

Sensitive Information—The loss, misuse, unauthorized access to, or modification of information that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. Section 522a (*The Privacy Act*), but that has not been specifically authorized under criteria established by an E.O. or an Act of Congress to be kept SECRET in the interest of the national defense or foreign policy. (See Air Force Directory [AFDIR] 33-303, *Compendium of Communications and Information Terminology.*)

Shareware—Privately or commercially developed software that users receive free of charge but pay a fee for continued or extended use. Normally, implied or promised support by the author is minimal or nonexistent. (See AFDIR 33-303.)

Software—A set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system (for example, compilers, library routines, and manuals).

User—The individual who operates the computer or uses application software.

Attachment 2

RELEASE OF SOFTWARE

A2.1. Software Reuse. It is HQ USAF policy to consider releasing specific software upon receiving a valid written request.

A2.1.1. Software is available from the Central Archive for Reusable Defense Software, the Defense Software Repository System, or the Air Force Defense Software Repository System. In such releases, the memorandum of agreement at paragraph **A2.3** need not be completed.

A2.1.2. As government furnished property software is available under the provisions of an acquisition contract. ***NOTE:*** When the government has unlimited rights in computer software in the possession of a contractor, the government will not pay for the use of such software in performance of government contracts or for the later delivery to the government of such computer software, provided that the contractor be entitled to compensation for converting the software into the prescribed form for reproduction and delivery to the government. In addition to adhering to the specific contract's provisions, the contractor also must sign the memorandum of agreement at paragraph **A2.3**

A2.1.3. Software is also available to organizations with which the Air Force does not have a contractual arrangement. In such situations, the recipient must sign the memorandum of agreement at paragraph **A2.3**

A2.2. Software Release or Disclosure. Each OPR bases the decision to release or disclose software on review of all significant factors including but not limited to, national security, militarily critical technology/dual use, royalty arrangements, potential for Air Force-industry CRADA, or pre-existing license agreement terms and conditions.

A2.2.1. In all software releases, the Air Force must ensure that it will not be held liable for any failure of the released software or its continued maintenance. This also applies to Air Force software deposited in all software reuse libraries. As such, the OPR must ensure that recipients of software from the reuse libraries understand this waiver of warranties and damages liability.

A2.3. Memorandum of Agreement: I/We the undersigned, on behalf of the Requesting Organization listed below (hereafter referred to as the "Requester"), request release of (software name) and understand and agree to the following:

a. NON-DISCLOSURE AGREEMENT. The Requester requests some or all of the following from _____ (insert the name of the specific Air Force organization or software reuse library): data, technical data, computer software, computer software documentation, computer programs, source code, firmware, and other information of like kind, type, or quality, either commercial or non-commercial, all of which may be subject to limited rights, restricted rights, government-purpose license rights, patents, copyrights, trade secret rights, or other confidential or proprietary constraints (collectively, the "Data"). In consideration therefore, the Requester agrees:

1) That the Data shall be used only for government, non-commercial, or non-profit purposes.

2) To strictly abide by and adhere to any and all restrictive markings placed on the Data, and the Requester shall not knowingly disclose or release the Data to third parties who are not engaged in work related to government, non-commercial, or non-profit purposes.

3) That any restrictive markings on the Data shall be included on all copies, modifications, and derivative works, or any parts or portions thereof; in any form, manner or substance, which are produced by the Requester including but not limited to incorporation of the Data into any other data, technical data, computer software, computer software documentation, computer programs, source code, or firmware, or other information of like kind, type or quality. In all such events, Requester shall clearly denote where such Data initiates and concludes by use of annotations or other standard markings.

4) That the government is entitled to royalty-free use of the Air Force-owned or -developed software that is released.

b. WAIVER OF WARRANTIES AND LIMITATIONS OF DAMAGES AGREEMENT. The requester and the Approving Authority agree that:

1) No guaranties, representations, or warranties either expressed or implied shall be construed to exist in any language, provision, or term contained in these materials or in any other documentation provided herewith (all such items are collectively referred to as the "Agreement"), and furthermore, the releasing organization disclaims and the requester waives and excludes any and all warranties of merchantability and any and all warranties of fitness for any particular purpose.

2) The Requester shall obtain from the releasing organization all of the "Data" (defined in the Non-Disclosure Agreement above), or any other products or services contemplated by the Agreement, in an "as is" condition.

3) The Requestor agrees to hold harmless and indemnify the Air Force against any and all loss, liability, cost or expense arising out of the use of any Data released under this agreement, to include, but not limited to, litigation costs or expenses.

c. The Requester's use of the Data shall not prevent the government from releasing the Data at any point in the future.

d. The Requester shall not offer the released Data or any modified version thereof for resale to the government, in whole or as part or subpart of a government deliverable, without explicitly stating that he is doing so by providing certification documentation (e.g., Section K of the Government Solicitation) to the contracting officer before contract award.

e. The Requester may use the released Data in a contract with the government, but understands that the government shall not pay the Requester for rights of use of such Data in performance of government contracts or for the later delivery to the government of such Data. The Requester may be entitled to compensation for converting, modifying, or enhancing the Data into another form for reproduction and delivery to the government, if authorized under a contract with the government.

f. The Requester is not entitled to any released Data that are subject to national defense security classification or the proprietary rights of others. The Requester shall report promptly the discovery of any such restricted Data to the USAF release approving authority below, and follow all instructions concerning the use, safeguarding, or return of such Data. The Requester shall not

copy, or make future study or use of any released Data later found to be subject to such restrictions.

g. As required, the Requester shall be responsible for compliance with any proscriptions on foreign disclosure of the released Data (contained, for example, in the Department of State International Traffic in Arms Regulations or the Department of Commerce Export Administration Regulations).

h. There may be a fee to cover the copying and shipping of the Data and any documentation.

i. The Requester and the Approving Authority intend that all agreements under this Memorandum of Agreement shall be governed by the laws of the United States of America.

NAME OF REQUESTOR AUTHORITY	NAME/TITLE OF USAF APPROVING
Requesting Organization/Address	Air Force Organization/Address
City, State, Zip Code	City, State, Zip Code
Signature of Requestor and Date	Signature of USAF Approving Authority and Date